CLAIMS

What is claimed is:

1. A system for enabling the preparation and secure management of an electronic document comprising:

a server processing unit and a server memory device electrically coupled to the server processing unit,

a client processing unit and a client memory device electrically coupled to the client processing unit,

a server program module, stored in the server memory device, for providing instructions to the server processing unit,

a client program module, stored in the client memory device, for providing instructions to the client processing unit, and

a communication medium, communicatively coupling the server processing unit and the client processing unit;

the client processing unit, responsive to the instructions of the client program module and the server processing unit, responsive to the instructions of the sever program module, being operative to:

authorize access to the system;

generate at least one electronic document;

prevent the creation of fraudulent versions of the electronic document;

allow electronic signatures to be associated with the electronic document; and

maintain an authoritative copy of the electronic document in the server memory device of the server processing unit.

2. The system of claim 1, further comprising an input device electrically coupled to the client processing unit, and wherein the client processing unit and the server processing unit are being operative to authorize access to the system by:

the client processing unit

receiving access information from the input device,

transmitting the access information to the server processing unit over the communication medium, and

receiving an authorized indicator from the server processing unit over the communications medium; and

the server processing unit

receiving the access information from the client processing unit over the communications medium,

verifying that the access information qualifies for granting access to the system, and

transmitting an authorized indicator to the client processing unit over the communications medium.

3. The system of claim 1, further comprising an input device electrically coupled to the client processing unit, and wherein the client processing unit and the server processing unit are operative to generate at least one electronic document by:

the client processing unit

receiving pertinent information from the input device, and

integrating the pertinent information into an electronic template.

4. The system of claim 3, wherein the electronic template includes predefined document information and a predefined document format, and the client processing unit and the server processing unit are operative to integrate the pertinent information into the electronic template by:

receiving a complete indicator from the input device, the complete indicator indicating that no additional pertinent information will be received by the client processing unit, and

merging the pertinent information and the predefined document information to generate the electronic document conforming to the predefined document format.

5. The system of claim 1, further comprising an input device electrically coupled to the client processing unit, and wherein the client processing unit and the server processing unit are operative to prevent the creation of fraudulent versions of the electronic document by the client processing unit, in response to generating the electronic document, rejecting any attempts to modify the electronic document.

6. The system of claim 1, further comprising an input device electrically coupled to the client processing unit; and wherein the client processing unit and the server processing unit are operative to prevent the creation of fraudulent versions of the electronic document by the client processing unit, in response to generating the electronic document, encrypting the electronic document and generating a signature key based at least in part on the contents of the electronic document.

7. The system of claim 1, further comprising an input device electrically coupled to the client processing unit, and the client processing unit and the server processing unit are operative to prevent the creation of fraudulent versions of the electronic document by:

the client processing unit,

in response to generating the electronic document, encrypting the electronic document, and

in response to an attempt to modify the electronic document, rendering the electronic document invalid.

8. The system of claim 1, further comprising an input device electrically coupled to the client processing unit, and wherein the client processing unit and the server processing unit are operative to allow electronic signatures to be associated with the electronic document by:

the client processing unit

receiving at least one signature input from the input device,

creating a signature file containing the signature input, and

encrypting the signature file using an encryption key that is based at least in part on the contents of the electronic document.

9. The system of claim 1, further comprising an input device electrically coupled to the client processing unit, and the client processing unit and the server processing unit are operative to maintain an authoritative copy of the electronic document in the server memory device of the server processing unit by:

the client processing unit

receiving a submit indicator from the input device, and

in response to receiving the submit indicator, transmitting the electronic document and the electronic signatures associated with the electronic document to the server processing unit over the communications medium; and

the server processing unit

receiving the electronic document and the electronic signatures,

preventing any modifications to the electronic document and the signature file, and

providing an unauthorized copy indicator on any electronic and hard copies of the electronic document, the unauthorized copy indicator indicating that the electronic and hard copies of the electronic document are not the authoritative copy of the electronic document.

10. A method for creating an electronic agreement and maintaining an authoritative copy of the electronic agreement, the method comprising the steps of:

(a) receiving a set of input information from an input source, the set of input information including a subset of information necessary to generate an electronic document;

(b) in response to receiving a complete indicator from the input source, the complete indicator indicating that the received subset of input information is complete, generating an electronic document by merging the subset of input information with a document template;

(c) receiving a set of electronic signatures from the input source, whereby upon receiving the set of electronic signatures, the electronic document is considered an electronic agreement; and

(d) in response to receiving a submit indicator, storing the electronic agreement within an access restricted computer system, the stored electronic agreement constituting an authoritative copy of the electronic agreement.

11. The method of claim 10, further comprising after the generating step, the step of providing a signature indicator to the input source, the signature indicator indicating that the generating step is complete and that the electronic document requires the input of the set of electronic signatures.

12. The method of claim 11, further comprising prior to the receiving a set of signatures step, the step of encrypting the electronic document.

13. The method of claim 12, further comprising after the encrypting step, the step of preventing the electronic document from being modified.

14. The method of claim 10, further comprising prior to the storing step, the step of encrypting the set of electronic signatures using an encryption key, the encryption key being based, at least in part, on the contents of the electronic document, whereby if the contents of the electronic document are modified, the electronic signatures and the electronic agreement will be invalid.

15. The method of claim 10, further comprising prior to the storing step, the step of providing an indicator that the set of electronic signatures has been received and that the electronic agreement is complete.

16. In a distributed computer system including at least one server device and at least one client device communicatively coupled to the server device, a method for maintaining an authoritative copy of an electronic agreement, the method comprising the steps of:

(a) a client device receiving a set of input information from an input source, the set of input information including a subset of information necessary to generate an electronic document and a set of signatures necessary to make the electronic document a binding agreement;

(b) the client device encrypting the electronic document using a first key and the set of signatures using a second key, the second key being based at least in part on the contents of the electronic document, whereby any modifications to the electronic document would result in invalidating the set of signatures;

(c) the client device transferring the encrypted electronic document and the encrypted set of signatures to a server device over a communications medium, the server device being access restricted, the stored electronic document and set of signatures constituting the only authoritative copy of the electronic agreement.

17. A client system operating within an electronic document system, the electronic document system including a server, a server memory storage device and a server program module, the client system comprising:

a client processing unit;

a client memory device, a display device and an input device all electrically coupled to the client processing unit;

a client program module, stored in the client memory device, for providing instructions to the client processing unit;

a communication medium, communicatively coupling the client system to the electronic document system; and

the client processing unit, responsive to the instructions of the client program module, being operative to:

authorize access to the electronic document system by

receiving access information from the input device,

transmitting the access information to the server over the communication medium, and

receiving an authorization indicator from the server processing unit over the communications medium;

generate at least one electronic document;

prevent the creation of fraudulent versions of the electronic document;

allow electronic signatures to be associated with the electronic document by

receiving a set of signatures from the input device,

creating at least one signature file containing the set of signatures, and

encrypting the signature file using an encryption key that is based at least in part on the contents of the electronic document; and

transfer the electronic document and the encrypted signature file to the server over the communications medium.

18. The client system of claim 17, wherein the client processing unit is operative to generate at least one electronic document by:

receiving pertinent information from the input device; and

merging the pertinent information with predefined document information to generate an electronic document conforming to a predefined document format.

19. The client system of claim 17 wherein the client processing unit is operative to prevent the creation of fraudulent versions of the electronic document by, after generating the electronic document, encrypting the electronic document and rejecting any attempts to enter additional pertinent information.

20. The system of claim 17 wherein the client processing unit is operative to prevent the creation of fraudulent versions of the electronic document by:

detecting an attempt to modify the electronic document, and

in response detecting an attempt, rendering the electronic document invalid.